533 Rec'd PCT/PTO 28 JUL 2000

FORM-PTO-1390 (Rev. 10-96) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 032326-080

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5): 09/601222 Unassigned

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR99/00096	20 January 1999	29 January 1998

TITLE OF INVENTION
SYSTEM AND METHOD FOR MANAGING COMPUTER APPLICATIONS SECURITY

APPLICANT(S) FOR DO/EO/US
Charles COULIER and Philippe BRUN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

533 Rec'd PCT/PTO 28 JUL 2000

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Unassigned 09/601222	PCT/FR99/00096	032326-080

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Search Report has been prepared by the EPO or JPO $840.00 (970)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) $670.00 (956)		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $690.00 (958)		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $970.00 (960)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $96.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 840.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)).	$ -0-	

Claims	Number Filed	Number Extra	Rate		
Total Claims	20 -20 =	-0-	X$18.00 (966)	$ -0-	
Independent Claims	2 -3 =	-0-	X$78.00 (964)	$ -0-	
Multiple dependent claim(s) (if applicable)			+$260.00 (968)	$ -0-	
TOTAL OF ABOVE CALCULATIONS =				$ 840.00	
Reduction for 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$ -0-	
SUBTOTAL =				$ 840.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)). +				$ -0-	
TOTAL NATIONAL FEE =				$ 840.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +				$ -0-	
TOTAL FEES ENCLOSED =				$ 840.00	
				Amount to be: refunded	$
				charged	$

a. ☒ A check in the amount of $ 840.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. 02-4800 in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

SIGNATURE

James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

(09/99)

Patent
Attorney's Docket No. 032326-080

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Charles COULIER et al	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: July 28, 2000	)	
	)	
For: SYSTEM AND METHOD FOR MANAGING COMPUTER APPLICATIONS SECURITY	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE SPECIFICATION:

Page 1, immediately following the title, insert the following:

--This disclosure is based upon, and claims priority from French Patent Application No. 98/01008, filed January 29, 1998, and International Application No. PCT/FR99/00096, filed January 20, 1999, the contents of which are incorporated herein by reference.

Background of the Invention--.

Page 3, before line 1, insert the following heading:

--**Summary of the Invention** --.

Page 4, before line 1, insert the heading:

--**Brief Description of the Drawing**--;

between lines 17 and 18, insert the heading:

--**Detailed Description**--.

IN THE CLAIMS:

1. (Amended) A system of managing the security of data processing applications, [characterised in that] comprising:

[-] directory files in which the data processing applications are stored, said [recorded in] directory files [(Repl, Rep2, Rep31, Rep32, Rep41, Rep42, Rep51, Rep52)] being organised in an n-level tree, the level 1 directory [(Repl)] being the highest level ; and

[-] a number [r] of security registers [(R)] which can each be allocated to a single directory [and], each security register [(R)] containing all the rights or secrets [Sl to Sp] which have been granted under a directory.

2. (Amended) A method of managing the security of data processing applications [in a system according to Claim 1, characterised in that it comprises the following steps consisting], comprising the steps of :

(a) storing in security registers [(R)] the rights [(Sl to Sp)] granted under a directory [(Rep)] according to given rules [(RG1, RG2, RG3)];

(b) seeking [in the tree] the secrets presented in an n-level tree of directory files in which data processing applications are stored; and

(c) verifying the knowledge of one or more rights at the level of the data processing application.

3. (Amended) A method according to Claim 2, [characterised in that] wherein the storage rules of step (a) are as follows :

[(RGI) :] allocation of a security register [(R)] to [the] a current directory as soon as a right has been granted under this directory or [the] said security register has been updated if a right has already been granted under this directory ;

[(RG2)] loss of the link connecting the old current directory to its security register when a new directory is selected except if the selected directory is the child of the old current directory; and

[(RG3)] allocating the security register that was allocated the earliest to the new current directory if the security registers are all allocated.

4. (Amended) A method according to Claim 2 [or 3, characterised in that] wherein step (b) consists of applying the following rule [consisting of]:

[(RG4)] verifying that the secret presented [(S)] is known in the current directory (Ni) or in a directory at a higher level.

5. (Amended) A method according to Claim 2, [3 or 4, characterised in that] wherein step (b) comprises the following intermediate steps [consisting of]:

(bl) seeking a secret in the current directory at level (Ni) and verifying the existence of the secret [(S)] within the application ;

(b2) if [this] said secret [(S)] exists, verifying that the presentation of the secret has succeeded ;

if the presentation has succeeded, the right associated with the secret [(S)] is granted at the level (Ni) of the current application ;

if the presentation has failed, the right associated with the secret [(S)] is not granted and the attempted presentation is terminated ;

(b3) if [this] said secret [(S)] does not exist within the current application at level (Ni) , seeking whether this secret [(S)] exists within the parent application at level N(i-1) ;

(b4) if [this] said secret [(S)] exists in the parent application at level [B]N(i-1), verifying that the presentation has succeeded ;

if the presentation has succeeded, the right associated with the secret [(S)] is granted in the current application at level (Ni) ;

if the presentation has failed, the right associated with the secret [(S)] is not granted and the attempted presentation is terminated ;

(b5) if the secret does not exist within the parent application at level N(i-1), seeking the existence of the secret [(S)] at the level of the application at level N(i-2) along the hierarchical axis and verifying that the presentation has succeeded ;

and so on as far as the highest hierarchical level as long as the existence of the secret [(S)] has not been discovered ;

(b6) if the secret [(S)] has not been discovered, the attempted presentation is terminated.

6. (Amended) A method according to [one of the preceding Claims 2 to 5, characterised in that] claim 2, wherein the step (c) consists of applying the following rule [consisting of]:

[(RG5)] authorisation of a function requiring knowledge of a secret [(S)] if and only if, running through the tree along the hierarchical axis from the current application to the root application, the first secret [(S)] is known to at least one of the applications belonging to the tree section for which the current application and the application containing the secret [(S)] are delimiters.

7. (Amended) A method according to [one of the preceding Claims 1 to 6, characterised in that] claim 2, wherein step (c) comprises the following steps [consisting of]:

(c1) verifying that a security register is associated with the current application at level Ni ;

(c2) authorising the function if the security register contains the required right and terminating the verification ;

(cl0) refusing the function and terminating the verification if the secret has not been discovered.

REMARKS

Entry of the foregoing amendments is respectfully requested. These amendments are intended to further clarify the language of the claims and specification.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: July 28, 2000

VERIFIED TRANSLATION OF INTERNATIONAL APPLICATION

I, Michele Ruby Gouze residing at 32 rue Arago, 92800 Puteaux, France, hereby certify that I am conversant with the French language and I am a competent translator thereof into the English language, and that to the best of my knowledge and belief, the following is a true and correct translation of the specification and claims as originally filed in respect of the International patent application PCT/FR99/00096 of the 20th January 1999.

Signed this 18TH day of July 2000

SYSTEM AND METHOD FOR MANAGING COMPUTER APPLICATIONS SECURITY

The invention concerns data processing systems and more particularly, in such systems, a system and method for managing the conditions for access to the different applications which are liable to be implemented by these data processing systems. The invention is preferentially but not limitatively intended to be implemented in the microprocessors of smart cards, whatever the field of use : health, banking, transport, mobile telephones etc.

The known security management methods have the following principal drawbacks :

- the first drawback is an obligation to have a hierarchy for selecting an application, that is to say it is necessary to pass through an imposed selection path commencing with the "grandparent" application and then the "parent" application in order to arrive at the "child" application, that is to say a selection path

similar to the one for selecting a file in a directory on a hard disk; in addition, no provision is made with regard to security.

There is therefore no relationship between the selection level and the security level.

- The second drawback is limiting the number of security levels or the number of applications. This is because a security register is dedicated to each application, the said register storing the rights acquired by this application through knowledge of secrets. In order to add n levels, that is to say to have a multiapplication series, it is necessary to associate, for example, a security register with each application, which results in using a large part of the high-speed memory where the security registers are stored. As the capacity of this high-speed memory is limited, it is not desirable to store many security registers therein. Thus, in certain systems, the number of hierarchical levels or the number of applications has been limited to three, that is to say three security registers.

- The third drawback is preventing the simple "emancipation" of the applications, that is to say making a "child" application independent of its "parent" application. This is because, when a new application is created, it is essential to use the rights and secrets of the "parent" application, which are the only ones available, until the secrets peculiar to the "child" application are created.

The aim of the present invention is to implement a method of managing the security of data processing applications which does not have the drawbacks disclosed above and which therefore makes it possible :

- not to be limited with regard to the number of hierarchical levels or number of applications, and ;

- to make a "child" application independent of the "parent" application without passing through the latter from the security point of view.

The invention therefore concerns a system of managing the security of data processing applications, characterised in that :

- the data processing applications are recorded in directory files organised in an n-level tree, the level 1 directory being the highest level, and ;

- a number r of security registers which can each be allocated to a single directory and each security register containing all the rights or secrets S1 to Sp which have been granted under a directory.

The invention also concerns a method of managing the security of data processing applications in the management system described above, characterised in that it comprises the following steps consisting of :

(a) storing in security registers the rights granted under a directory according to given rules ;

(b) seeking in the tree the secrets presented, and

(c) verifying the knowledge equivalent to one or more rights at the level of the data processing application in order to satisfy the access conditions.

Other characteristics and advantages of the present invention will emerge from a reading of the following description of particular example embodiments, the said description being given in relation to the accompanying drawings, in which :

- Figure 1 is an example of a directory tree structure ;

- Figures 2.1 to 2.14 illustrate examples of the application of three rules for the allocation or deallocation of a security register to or from a directory ;

- Figures 3.1a to 3.6a and 3.1b to 3.6b illustrate examples of the application of the rule for the presentation of a secret ; and

- Figures 4.1 to 4.6 illustrate examples of the application of the rule for verifying the granting of the required right.

The invention will be described in its application to a smart card and, more precisely, to a microprocessor used in a smart card. However, it is also applicable to any data processing system where it is necessary or simply desirable for certain services or functions offered by the system to be accessible only to certain users or operators.

In the case of smart cards, for example a bank card or a mobile telephone card, the services or functions which are available to the user may be subject to authorisation according to the type of subscription taken out, these authorisations (or rights) being granted by proving the knowledge of secrets which allow

access to the files necessary for the use of the service or function.

In the remainder of the description, the following definitions will be adopted :

- A file is a set of data able to be protected by access conditions ;

- A directory Rep is a set of files and/or directories in accordance with an arborescent organisation (Figure 1); normally a directory is dedicated solely to one application ;

- The conditions for access to a file or directory Rep define the criteria to be fulfilled, such as the presentation of a secret code or an external authentication, in order to be able to effect such or such a function on the file or directory ;

- The files and directories are organised in a tree with several levels, where the highest-level directory (level 1) is referred to as the "root" directory, or root of the tree. A level characterises the directories having the same hierarchical degree. The use of directories makes it possible to structure the data in a smart card. In Figure 1, only the directories Rep1, Rep2, Rep31, Rep32, Rep41, Rep42, Rep51 and Rep52 have been presented and each can contain one or more files. The directory Rep1 is the root of the tree comprising n=5 levels of directories, the directories Rep41 and Rep42 belonging to the level i=4 ;

- A security register R contains all the rights which have been granted under a directory and a right is the proof of the knowledge of a secret which is

identified by a reference such as a name, a number or an identifier. There are several ways of proving knowledge of a secret, for example by exchanging the value of the secret between the terminal and smart card or by exchanging data calculated by means of this secret: the operation is called presentation of the secret.

In general terms, the foundation of security on a smart card is to be able to make the use of the service or the function of the smart card dependent on proof of the knowledge of one or more secrets. Thus, in order to be able to use a function of the card, it is necessary :

- for the smart card to previously store this proof of the knowledge of the secret or secrets in a security register ;

- for the bearer of the smart card or terminal to prove that he has knowledge of the secret or secrets protecting the function ;

- for the card to verify, when the function is used, that the secret or secrets are indeed known.

The invention lies in the steps of the method consisting of :

(a) storing in the smart card the knowledge of the secret or secrets, that is to say the rights granted, according to the rules of allocation and deallocation of a security register to a directory ;

(b) seeking in the tree the secret or secrets presented ;

(c) verifying the knowledge of the secret or secrets in order to fulfil the access conditions.

To store the knowledge of a secret in a smart card (step (a)), it is necessary to correctly present the secret, which amounts to proving that the outside, for example a terminal or a card carrier, has knowledge of the said secret, this knowledge conferring on it or him the right to use functions or services offered by the card. It is the right which is stored in a security register at the rate of one register per application.

A security register R comprises a number p of digits or positions, each position being allocated to the knowledge of a secret corresponding to a granted right. A register with p=8 positions can record the knowledge of eight secrets S1 to S8, which will correspond to eight rights granted.

The number r of security registers R can be any number and the example which will be described will include r=3 of them. The security registers are not dedicated to a given level or directory as in the prior art and the link between a directory and a security register is dynamic, that is to say this link can be created or broken in accordance with the rules of the method according to the invention.

In order to store a right in a directory, it is necessary first of all to allocate or deallocate a security register to or from a directory in accordance with the following three rules RG1 to RG3 :

Rule RG1 :

A register is allocated to the current directory as soon as a right is granted under this directory, for example a secret code or an authentication. If a right

has already been granted under this directory, the register dedicated to it is updated.

Rule RG2 :

Selection of a new directory gives rise to the loss of the link connecting the old current directory to its security register except if the directory selected is the "child" of the old current directory.

Rule RG3 :

If the number r of security registers is saturated, that is to say the R=3 in the example described are used, the register which was allocated first, that is to say the highest level in the tree, is allocated to the new current directory in accordance with rule RG1.

It should be noted that the application of rule RG2 makes it possible to allocate two security registers to the same level, so that the allocation of a security register to a directory may be represented by a hierarchical level Ni allocated to the security register concerned, i varying from 1 to n.

Figures 2.1 to 2.14 illustrate applications of the rules RG1, RG2 and RG3. In these figures and the others, a black circle designates a directory, a grey circle designates a selected directory and a white circle designates a selected directory with a right removed.

Figure 2.1 illustrates the absence of selection of a directory whilst Figures 2.2 and 2.3 illustrate respectively the selection of the directories Rep1 and Rep2.

Thus the application of rule RG1 is illustrated in Figures 2.4, 2.6, 2.8, 2.10, 2.12 and 2.14. Figure 2.4 illustrates the presentation of a secret under the directory Rep2 at level N2. Figure 2.6 illustrates the presentation of a secret under the directory Rep31 at level N3. Figure 2.8 illustrates the presentation of a right under the directory Rep41 at level N4. Figure 2.10 illustrates the presentation of a right under the directory Rep51 at level N5. Figure 2.12 illustrates the presentation of a right under the directory Rep41. Figure 2.14 illustrates the presentation of a right under the directory Rep42.

The application of rule RG2 is illustrated by Figures 2.5, 2.7 and 2.9 with regard to the maintenance of the link between a security register and its directory when a new "child" directory thereof is selected.

Figures 2.5, 2.7 and 2.9 illustrate respectively the selection of the directory Rep31, Rep41 or Rep51.

The application of rule RG2 is illustrated by Figures 2.11 and 2.13 with regard to the breaking of the link between a security register and its directory. Thus Figure 2.11 illustrates the selection of the directory Rep41 whilst Figure 2.13 illustrates the selection of the directory Rep42.

The application of rule RG3 is illustrated by Figure 2.10, in which the register allocated the earliest R1 is allocated to the new selected directory Rep51.

Step (a) consisting of storing the rights attached to the knowledge of the secrets being performed, step (b) consisting of seeking in the tree the secret presented by the bearer of the smart card or by the terminal can be implemented.

A secret presented at the level of an application confers a right of use at the level of this same application. Thus the successful presentation of a secret within an application with the hierarchical level Ni updates the security register dedicated to this hierarchical level, in accordance with rule RG1, even if the secret presented is physically situated in a higher hierarchical level.

The rule for presentation of a secret is as follows :

Rule RG4 :

The presentation of a reference secret S amounts to verifying that the bearer of the smart card or terminal knows the value of the first reference secret S found by running through the hierarchical axis of the current application to the root directory.

The presentation of the reference secret S at the level of the current application situated at the hierarchical level Ni is effected by means of the following intermediate steps consisting of :

(b1) seeking a reference secret S in the current directory, that is to say at the level Ni, by means of a security management system, and verifying the existence of this secret within the application ;

(b2) if this secret exists, verifying that the presentation of the secret has succeeded, for example value for a secret code, cryptogram for a key, etc.

If the presentation has succeeded, the right associated with reference secret S is granted at the level of the current application at level Ni.

If the presentation has failed, the right associated with the reference secret S is not granted and the attempted presentation is terminated.

(b3) If the reference secret S does not exist within the current application at level Ni, seeking whether a secret with the same reference exists within the parent application at a level N(i-1) of the current application.

(b4) If the secret exists at the level of the parent application at level N(i-1), verifying that the presentation has succeeded.

If the presentation has succeeded, the right associated with the reference secret S is granted at the level of the current application at level Ni.

If the presentation has failed, the right associated with the reference secret S is not granted and the attempted presentation is terminated.

(b5) If the reference secret S does not exist within the parent application at level N(i-1), seeking the reference secret S at level N(i-2) along the hierarchical axis, and so on as long as the existence of a reference secret S has not been discovered.

(b6) If the reference secret S has not been found, the attempted presentation is terminated.

Several examples of the application of rule RG4 are illustrated in Figures 3.1a to 3.6a and 3.1b to 3.6b. Figures 3.1a and 3.1b, 3.2a and 3.2b, 3.3a and 3.3b correspond to examples where the right is granted whilst Figures 3.4a and 3.4b, 3.5a and 3.5b, 3.6a and 3.6b correspond to examples where the right is not granted.

In Figure 3.1a, the secret S3 exists locally under the directory Rep41 and no register is allocated to the directory Rep41. In Figure 3.1b, knowledge of the secret S3 is proved; a register R3 is allocated to the directory Rep41 at level N4 and the right is granted.

In Figure 3.2a, the secret S3 exists locally under the directory Rep41 and a register R3 is already allocated to the directory Rep41. Knowledge of the secret S3 is therefore proved and the security register R3 allocated to the directory Rep41 is updated (S3) so that the right is granted (Figure 3.2b).

In Figure 3.3a, the secret S2 does not exist locally under the directory Rep41; a register R3 is already allocated to the directory Rep41 and a secret S2 exists at the same time under the directories Rep2, Rep1, Rep42 and Rep51. Knowledge of the secret S2 is therefore proved and the security register allocated to the directory Rep41 is updated so that the right is granted (Figure 3.3b).

In Figure 3.4a, the secret S2 does not exist locally under the directory Rep41; a register R3 is already allocated to the directory Rep41 and a secret S2 exists both under the directories Rep2, Rep1, Rep42 and

Rep51. Knowledge of the secret S2 is therefore not proved so that the security register R3 allocated to the directory Rep41 is not updated and the right is not granted (Figure 3.4b).

In Figure 3.5a, the secret S2 does not exist locally under the directory Rep41; a register R3 is already allocated to the directory Rep41 and a secret S2 exists at the same time under the directories Rep2, Rep1, Rep42 and Rep51. Knowledge of the secret S2 is therefore not approved so that the security register R3 allocated to the directory Rep41 is not updated and the right is not granted (Figure 3.5b).

In Figure 3.6a, the secret S2 does not exist locally under the directory Rep41; a register R3 is already allocated to the directory Rep41 and a secret S2 exists at the same time under the directories Rep2, Rep1, Rep42 and Rep51. Knowledge of the secret S2 is not proved so that the security register R3 allocated to the directory Rep41 is not updated and the right is not granted (Figure 3.6b).

Step (c) consists of verifying that knowledge of the secret or secrets for fulfilling the access conditions, that is to say verifying that the secret protecting use of a function and service of the smart card, is indeed known to the outside world, that is to say that the right required has indeed been granted.

To this end, the invention implements a fifth rule RG5 which is stated as follows:

Rule RG5 :

A function requiring knowledge of a secret S is authorised if and only if, running through the tree along the hierarchical axis of the current application towards the root application, the first secret S encountered is known, that is to say correctly presented, by at least one of the applications belonging to the tree section having the current application and the application containing the secret S as its delimiters, these applications being able to be merged if the secret S exists in the current application.

In order to perform step (c), the management system must perform the following steps consisting of :

(c1) verifying that a security register is associated with the current application at level Ni ;

(c2) authorising the function if the security register contains the required right and terminating the verification ;

(c3) seeking the existence of the reference secret S within the current application at level Ni if no security register is associated with the current application or if the associated register does not contain the required right ;

(c4) refusing the function and terminating the verification if the secret exists within the current application ;

(c5) verifying that a security register is associated with the parent application at level N(i-1) of the current application if the reference secret S does not exist within the current application at level Ni ;

(c6) authorising the function and terminating the verification if the security register associated with the parent application contains the right required for using the function ;

(c7) seeking the existence of the reference secret S within the parent application at level N(i-1) of the current application if no security register is associated with the parent application or if the associated security register does not contain the required right ;

(c8) refusing the function and terminating the verification if the reference secret S exists within the parent application at level N(i-1) ;

(c9) verifying that a security register is associated with the grandparent application at level N(i-2) of the current application along the hierarchical axis of the current application towards the root application, if the reference secret S does not exist within the parent application at level N(i-1),

and so on as long as the existence of the reference secret S has not been discovered ;

(c10) refusing the function and terminating the verification if the secret has not been discovered.

Figures 4.1 and 4.2 illustrate two examples of an authorised function whilst Figures 4.3, 4.4, 4.5 and 4.6 illustrate four examples of a refused function.

In Figure 4.1, the function is accepted since the secret S3 exists locally, and is known under the directory Rep41.

In Figure 4.2, the function is accepted since the secret S1 does not exist locally but is known under the directory Rep2.

In Figure 4.3, the function is rejected since the secret S3 exists locally under the directory Rep41 and no right has been granted under this directory.

In Figure 4.4, the function is rejected since the secret S3 exists locally under the directory Rep41 and, although a security register R3 is allocated to the directory Rep41, knowledge of the secret S3 has not been proved.

In Figure 4.5, the function is rejected since the secret S2, which does not exist locally under the directory Rep41, nor in the directory Rep31, exists under the directory Rep2 and no security register is allocated to the directory Rep2. It should be noted that the function is rejected although a secret S2 is known under the directory Rep1.

In Figure 4.6, the function is rejected since the secret S1 has not been found by running along the hierarchical axis from the directory Rep41 towards the directory Rep1, although a secret S1 exists under the directories Rep51 and Rep32.

CLAIMS

1. A system of managing the security of data processing applications, characterised in that :

- the data processing applications are recorded in directory files (Rep1, Rep2, Rep31, Rep32, Rep41, Rep42, Rep51, Rep52) organised in an n-level tree, the level 1 directory (Rep1) being the highest level ; and

- a number r of security registers (R) which can each be allocated to a single directory and each security register (R) containing all the rights or secrets S1 to Sp which have been granted under a directory.

2. A method of managing the security of data processing applications in a system according to Claim 1, characterised in that it comprises the following steps consisting of :

(a) storing in security registers (R) the rights (S1 to Sp) granted under a directory (Rep) according to given rules (RG1, RG2, RG3) ;

(b) seeking in the tree the secrets presented ; and

(c) verifying the knowledge of one or more rights at the level of the data processing application.

3. A method according to Claim 2, characterised in that the storage rules of step (a) are as follows :

(RG1) : allocation of a security register (R) to the current directory as soon as a right has been granted under this directory or the said security

register has been updated if a right has already been granted under this directory ;

(RG2) loss of the link connecting the old current directory to its security register when a new directory is selected except if the selected directory is the child of the old current directory ;

(RG3) allocating the security register allocated the earliest to the new current directory if the security registers are all allocated.

4. A method according to Claim 2 or 3, characterised in that step (b) consists of applying the following rule consisting of :

(RG4) verifying that the secret presented (S) is known in the current directory (Ni) or in a directory at a higher level.

5. A method according to Claim 2, 3 or 4, characterised in that step (b) comprises the following intermediate steps consisting of :

(b1) seeking a secret in the current directory at level (Ni) and verifying the existence of the secret (S) within the application ;

(b2) if this secret (S) exists, verifying that the presentation of the secret has succeeded ;

if the presentation has succeeded, the right associated with the secret (S) is granted at the level (Ni) of the current application ;

if the presentation has failed, the right associated with the secret (S) is not granted and the attempted presentation is terminated ;

(b3) if this secret (S) does not exist within the current application at level (Ni), seeking whether this secret (S) exists within the parent application at level N(i-1) ;

(b4) if this secret (S) exists in the parent application at level B(i-1), verifying that the presentation has succeeded ;

if the presentation has succeeded, the right associated with the secret (S) is granted in the current application at level (Ni) ;

if the presentation has failed, the right associated with the secret (S) is not granted and the attempted presentation is terminated ;

(b5) if the secret does not exist within the parent application at level N(i-1), seeking the existence of the secret (S) at the level of the application at level N(i-2) along the hierarchical axis and verifying that the presentation has succeeded ;

and so on as far as the highest hierarchical level as long as the existence of the secret (S) has not been discovered ;

(b6) if the secret (S) has not been discovered, the attempted presentation is terminated.

6. A method according to one of the preceding Claims 2 to 5, characterised in that the step (c) consists of applying the following rule consisting of :

(RG5) authorisation of a function requiring knowledge of a secret (S) if and only if, running through the tree along the hierarchical axis from the current application to the root application, the first

secret (S) is known to at least one of the applications belonging to the tree section for which the current application and the application containing the secret (S) are delimiters.

7. A method according to one of the preceding Claims 1 to 6, characterised in that step (c) comprises the following steps consisting of :

(c1) verifying that a security register is associated with the current application at level Ni ;

(c2) authorising the function if the security register contains the required right and terminating the verification ;

(c3) seeking the existence of the reference secret S within the current application at level Ni if no security register is associated with the current application or if the associated register does not contain the required right ;

(c4) refusing the function and terminating the verification if the secret exists within the current application ;

(c5) verifying that a security register is associated with the parent application at level N(i-1) of the current application if the reference secret S does not exist within the current application at level Ni ;

(c6) authorising the function and terminating the verification if the security register associated with the parent application contains the right required for using the function ;

(c7) seeking the existence of the reference secret S within the parent application at level N(i-1) of the current application if no security register is associated with the parent application or if the associated security register does not contain the required right ;

(c8) refusing the function and terminating the verification if the reference secret S exists within the parent application at level N(i-1) ;

(c9) verifying that a security register is associated with the grandparent application at level N(i-2) of the current application along the hierarchical axis of the current application towards the root application, if the reference secret S does not exist within the parent application at level N(i-1) ;

and so on as long as the existence of the reference secret S has not been discovered ;

(c10) refusing the function and terminating the verification if the secret has not been discovered.

SYSTEM AND METHOD FOR MANAGING COMPUTER APPLICATIONS SECURITY

ABSTRACT

The invention concerns a system for managing computer applications security, characterised in that : The computer applications are recorded in directory files (Rep1, Rep2, Rep31, Rep32, Rep41, Rep42, Rep51, Rep52) organised in a tree-like structure with n levels, level 1 directory (Rep1) being the highest level ; a number r of security registers (R) being attributed each to one single directory and each security register (R) containing the set of rights or secrets S1 to Sp which have been assigned under one directory.

FIG.2.1

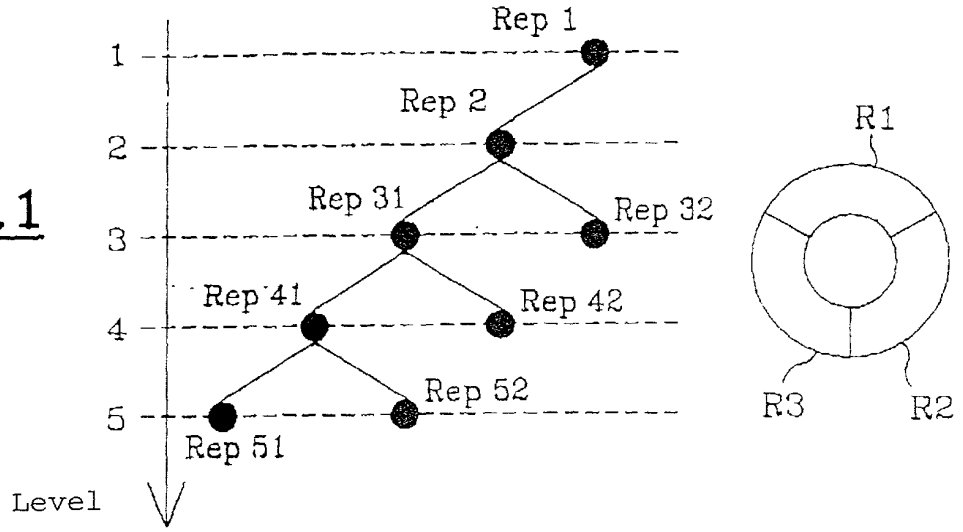


FIG.2.2

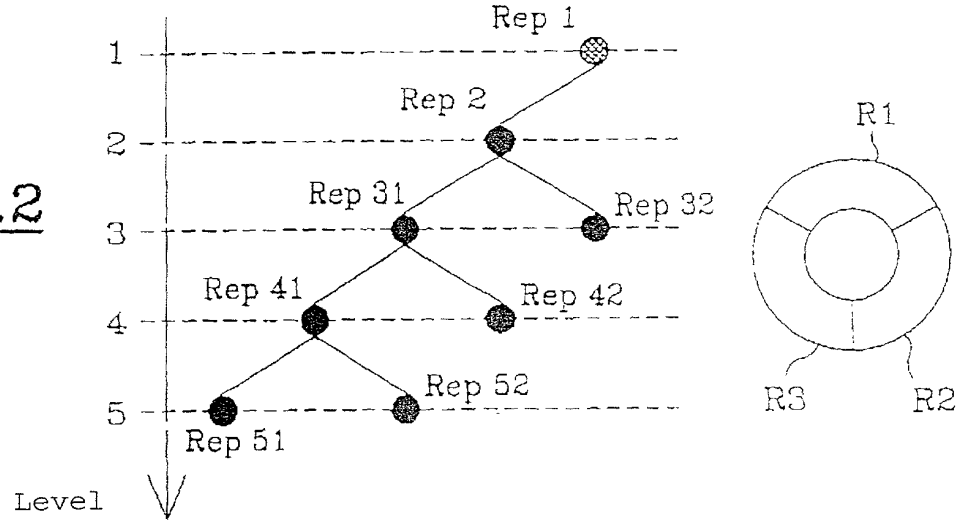


FIG.2.3

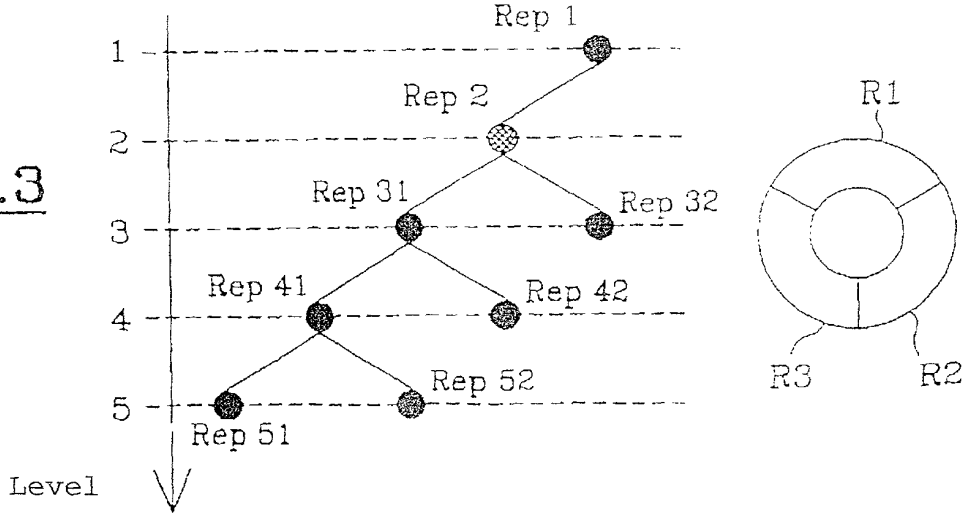


FIG.2.4

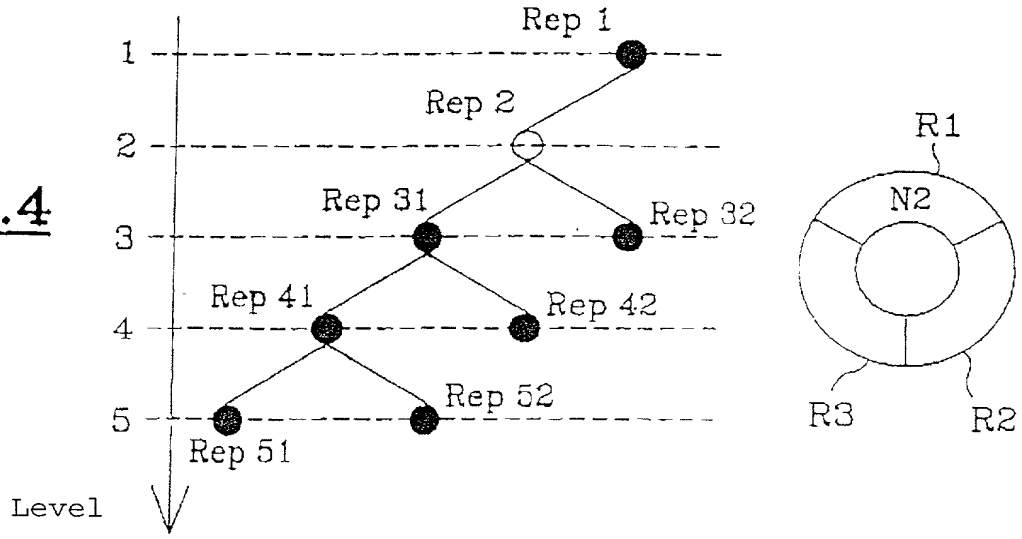


FIG.2.5

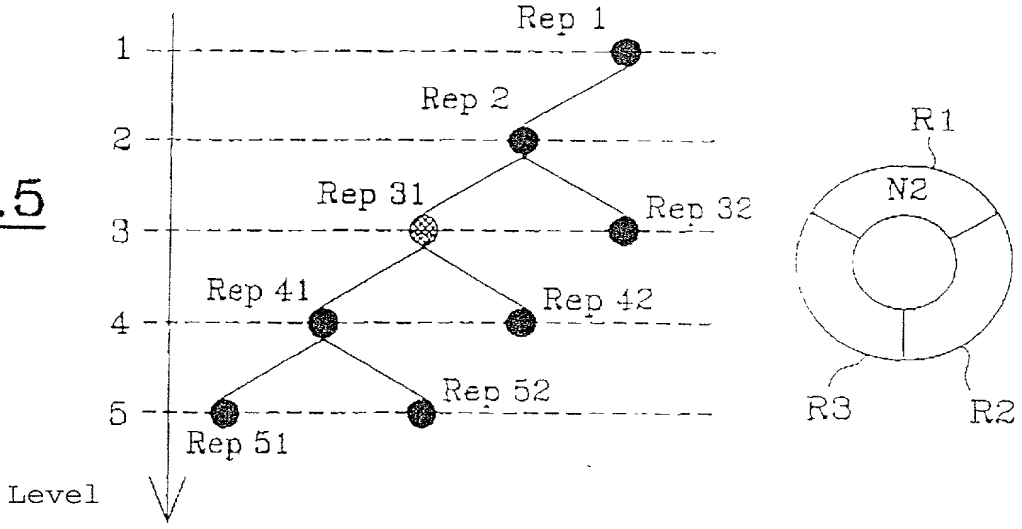


FIG.2.6

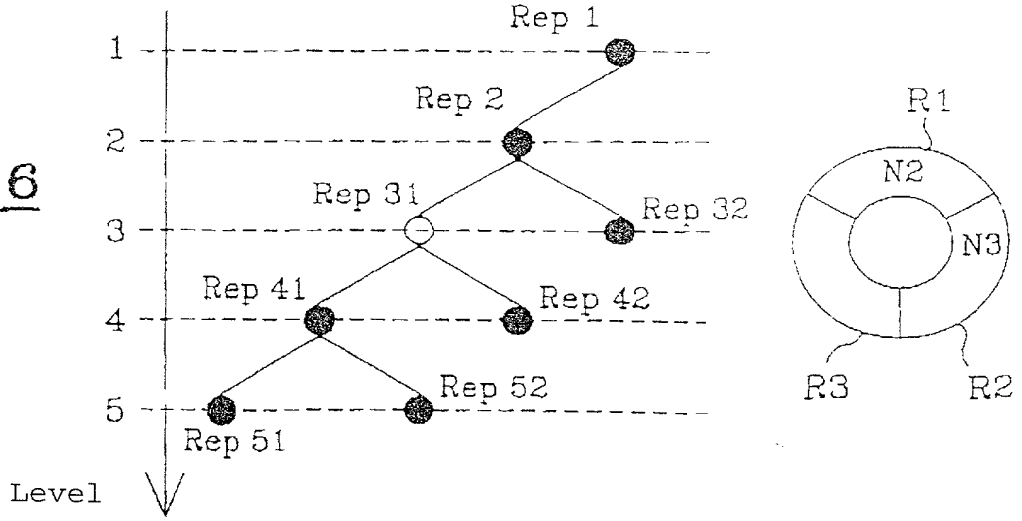


FIG.2.7

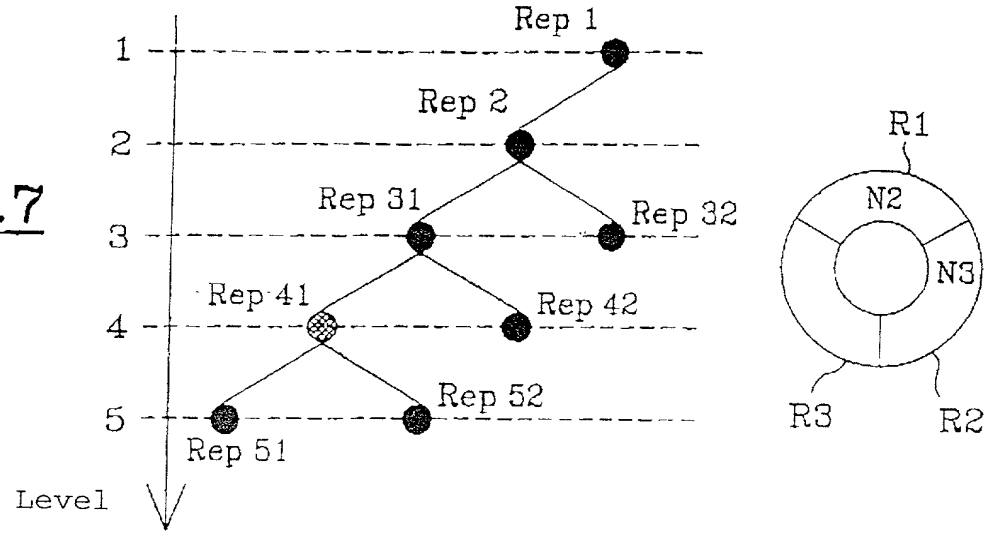


FIG.2.8

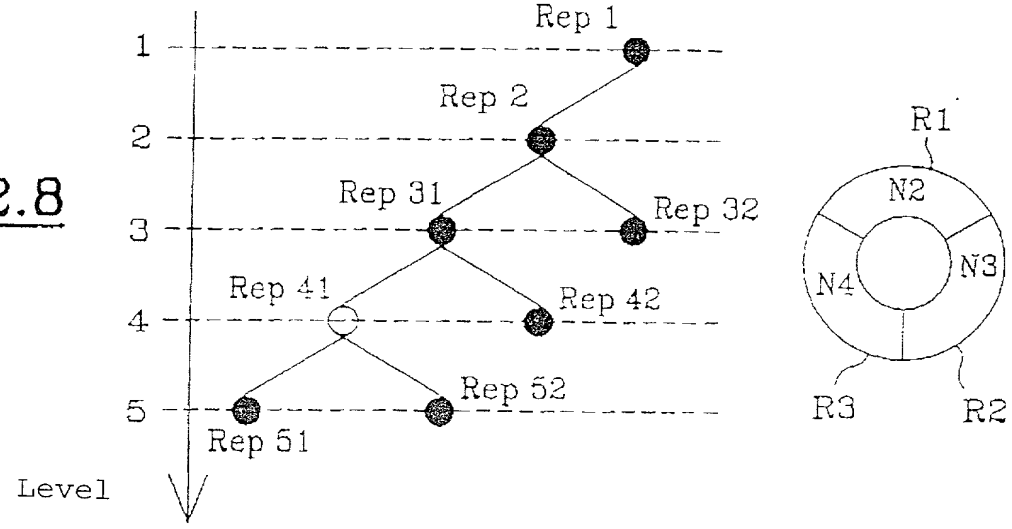


FIG.2.9

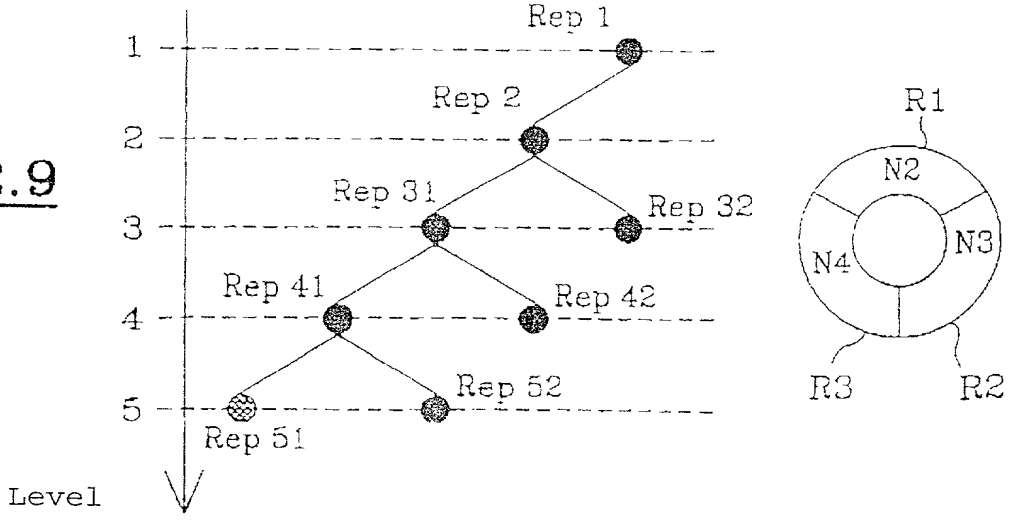


FIG.2.10

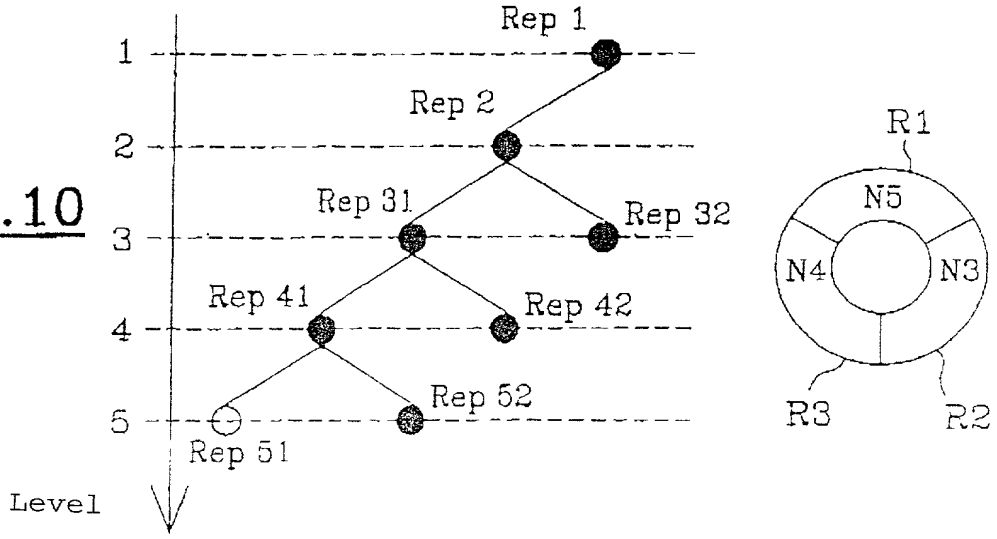


FIG.2.11

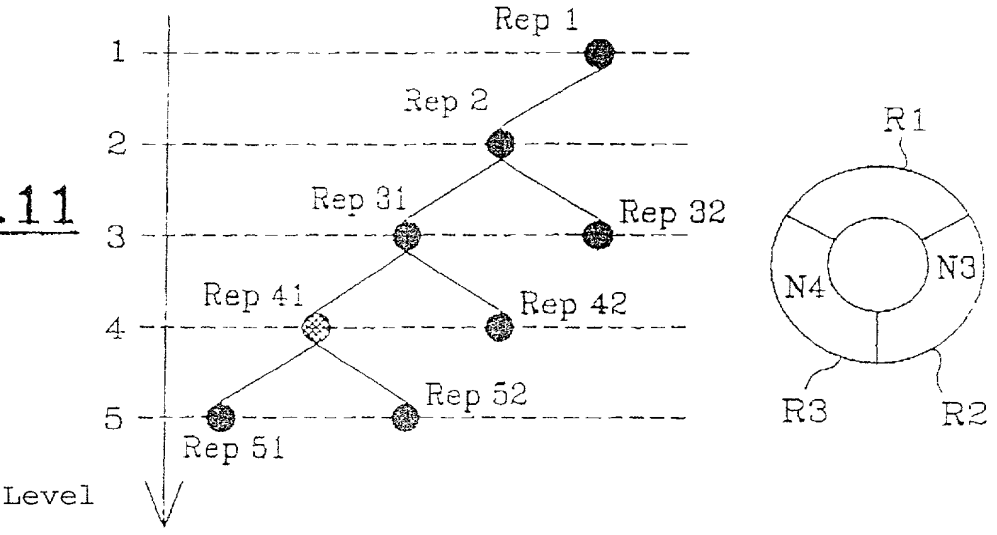


FIG.2.12

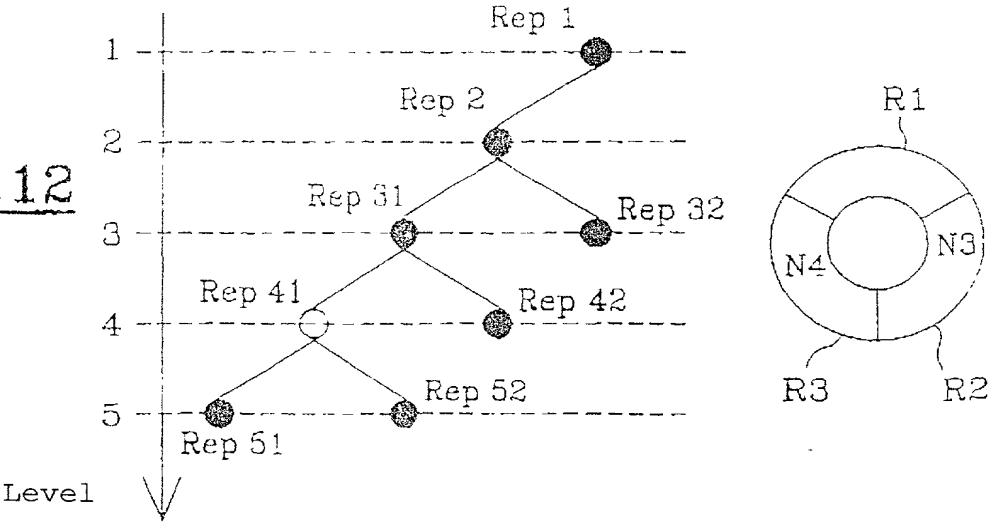


FIG.2.13

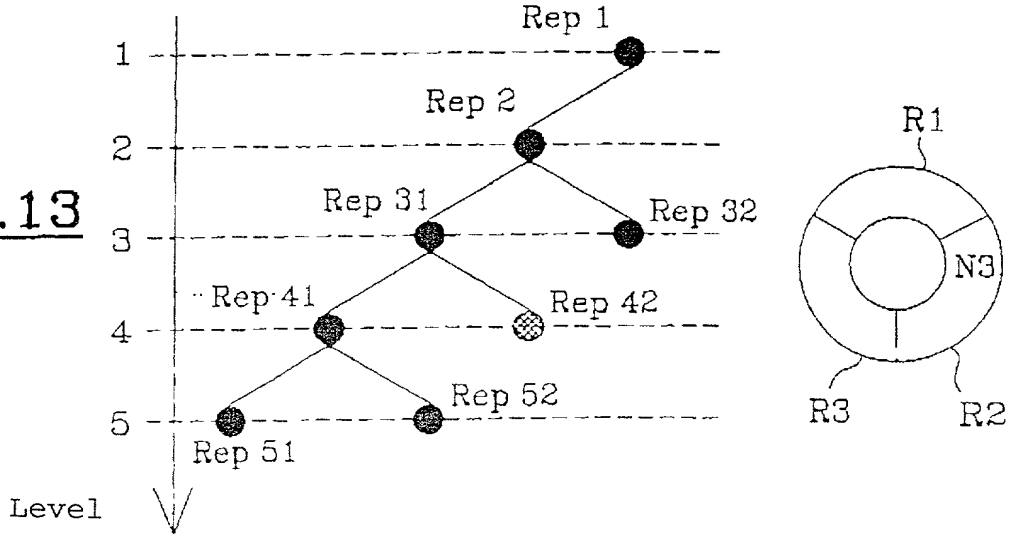


FIG.2.14

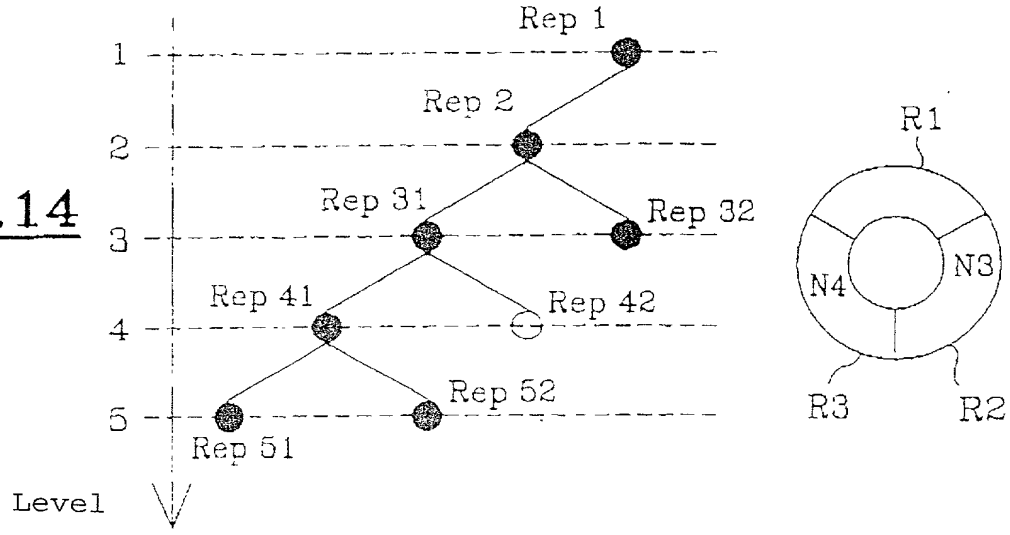


FIG.1

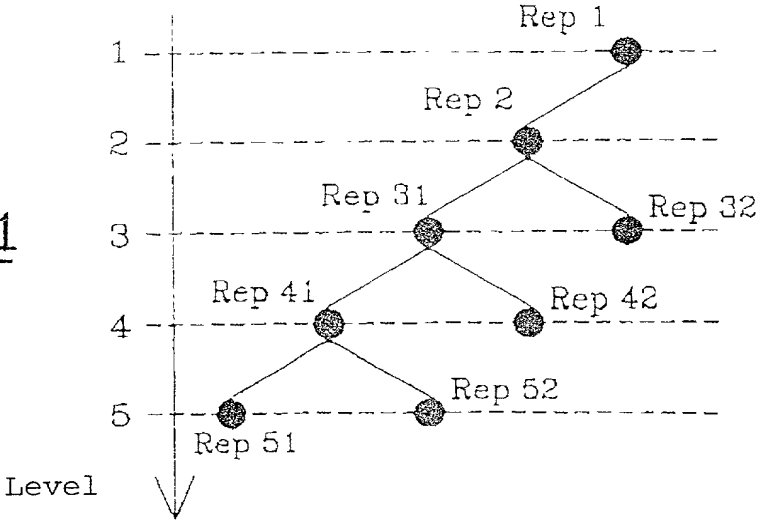


FIG.3.1a

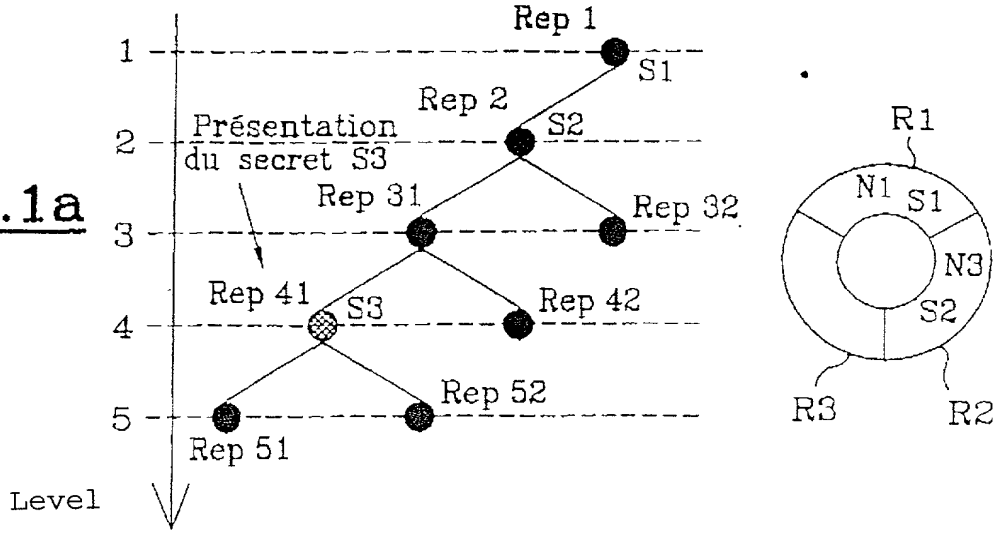


FIG.3.1b

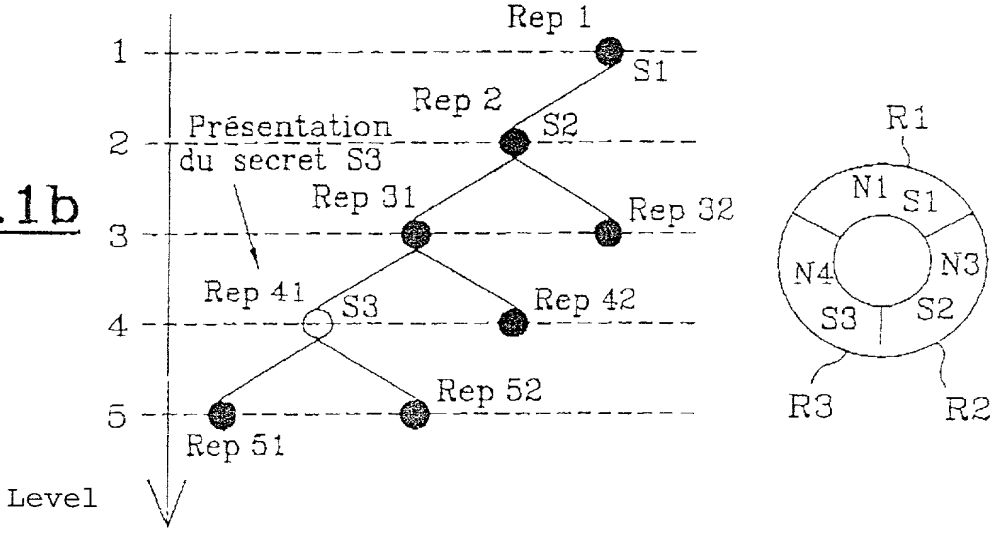


FIG.3.2a

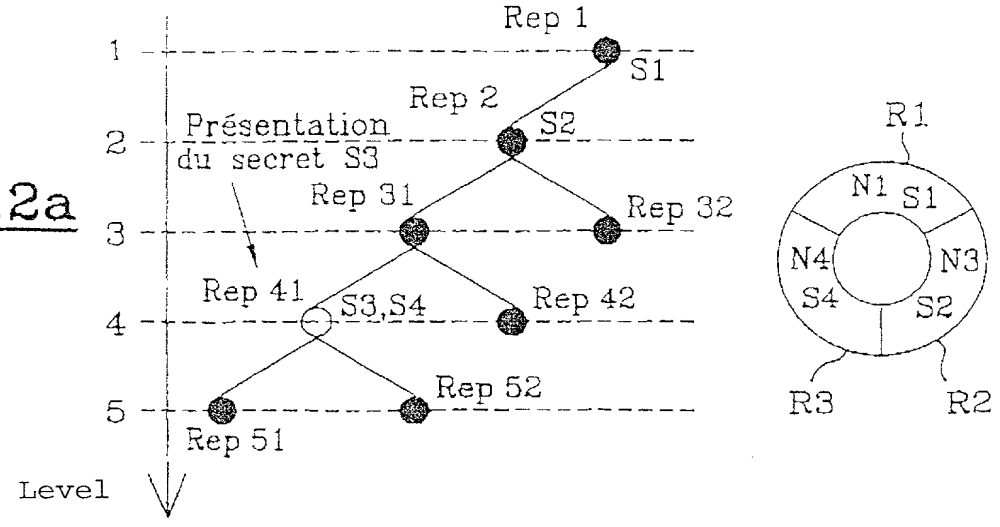


FIG.3.2b

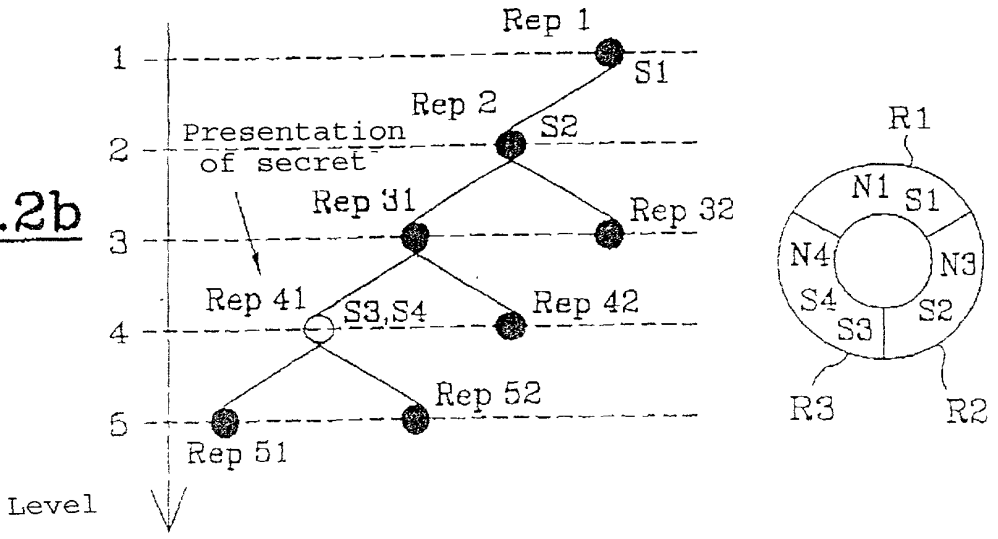


FIG.3.3a

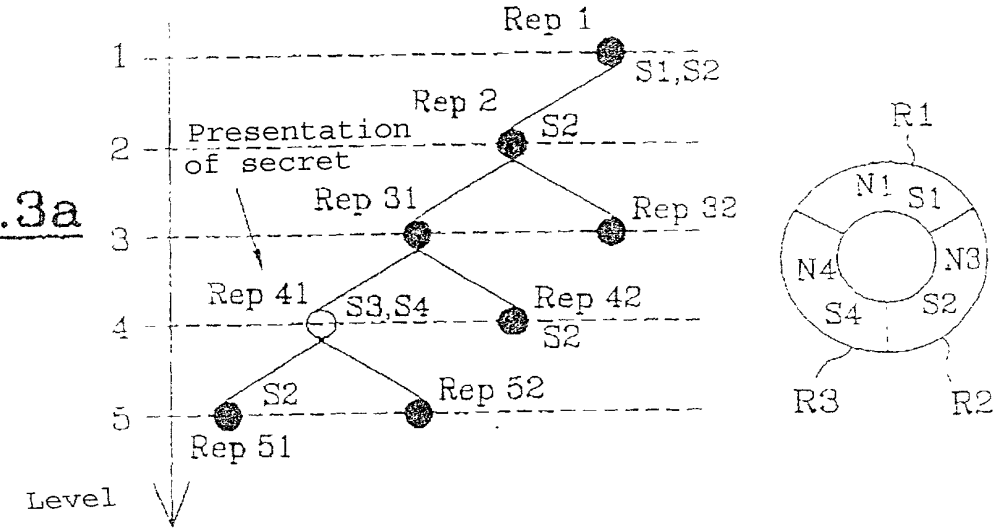


FIG.3.3b

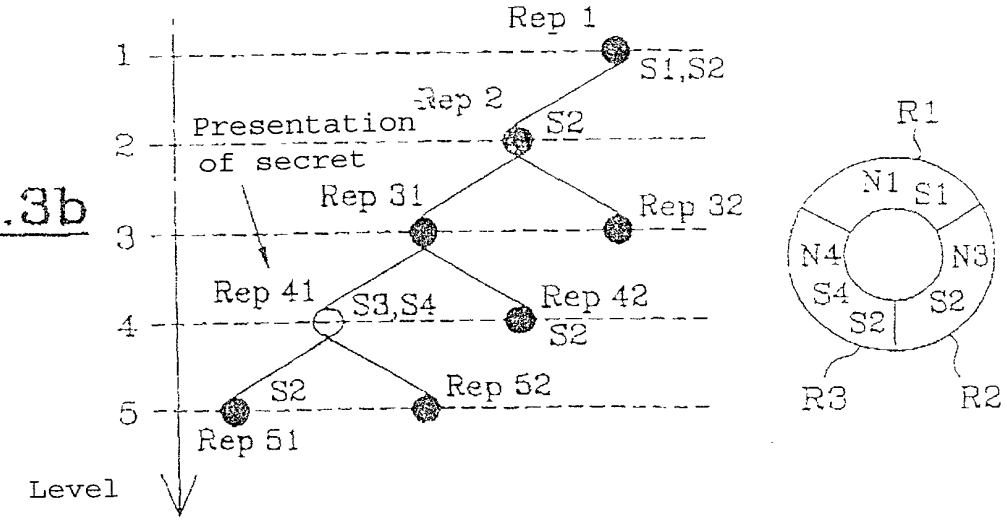


FIG.3.4a

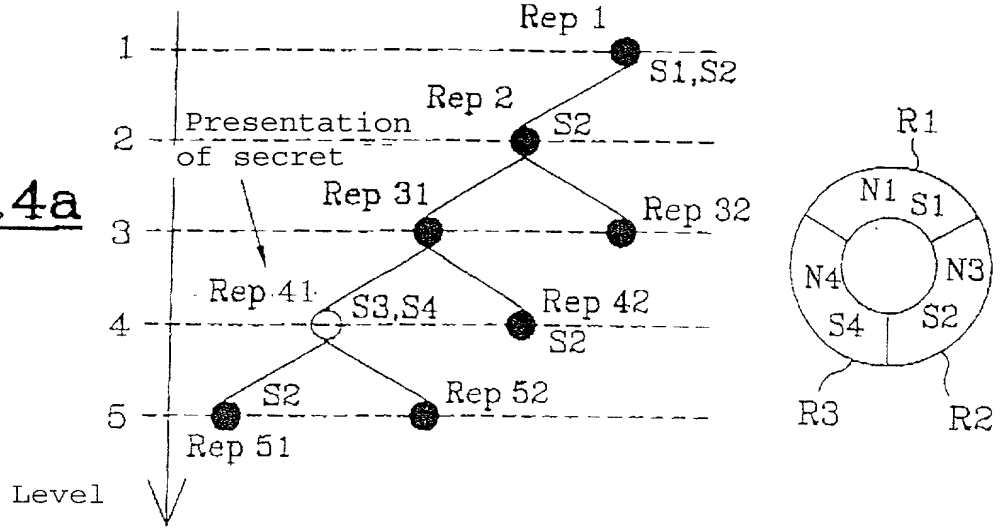


FIG.3.4b

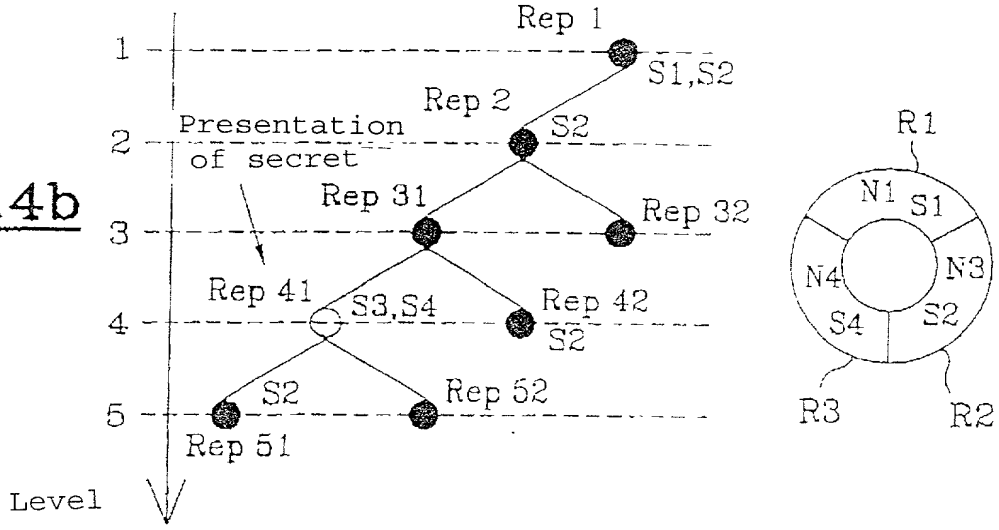


FIG.3.5a

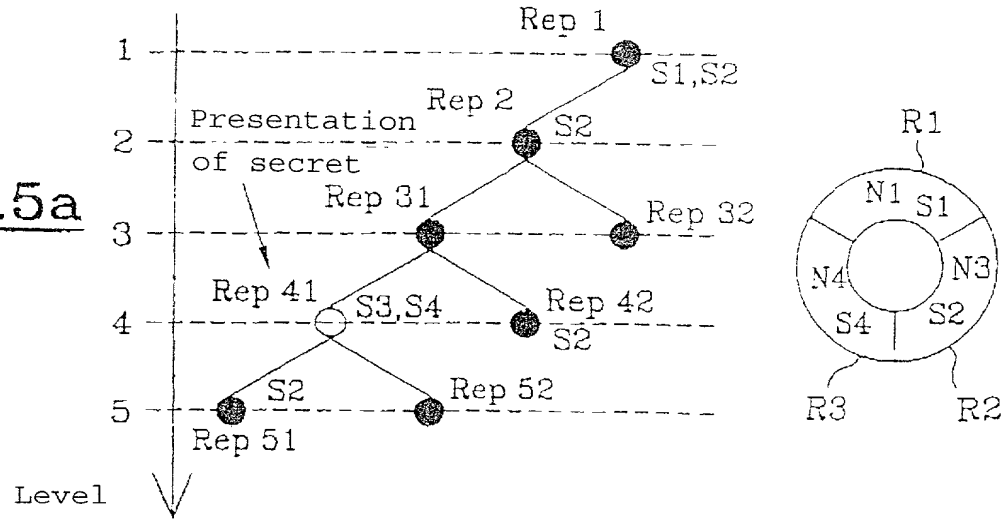


FIG.3.5b

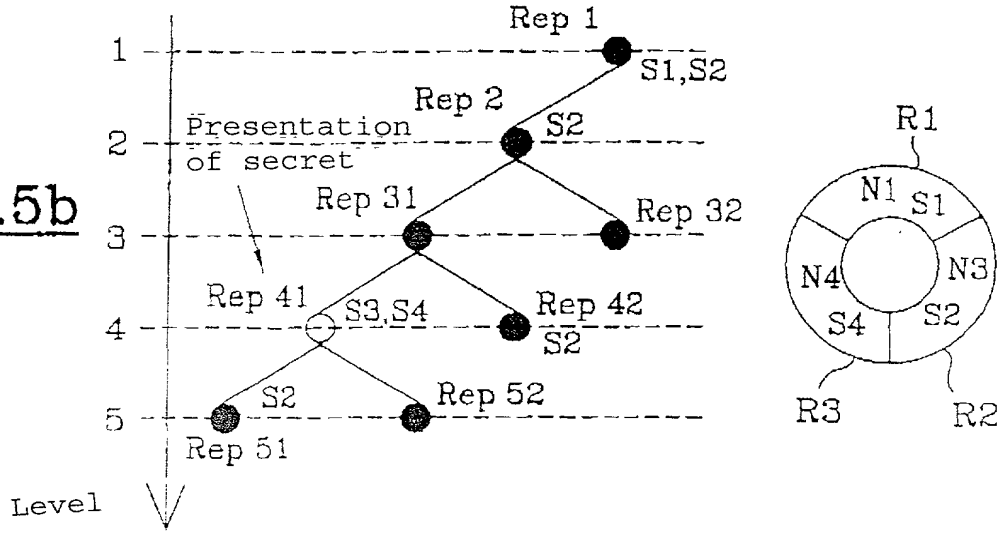


FIG.3.6a

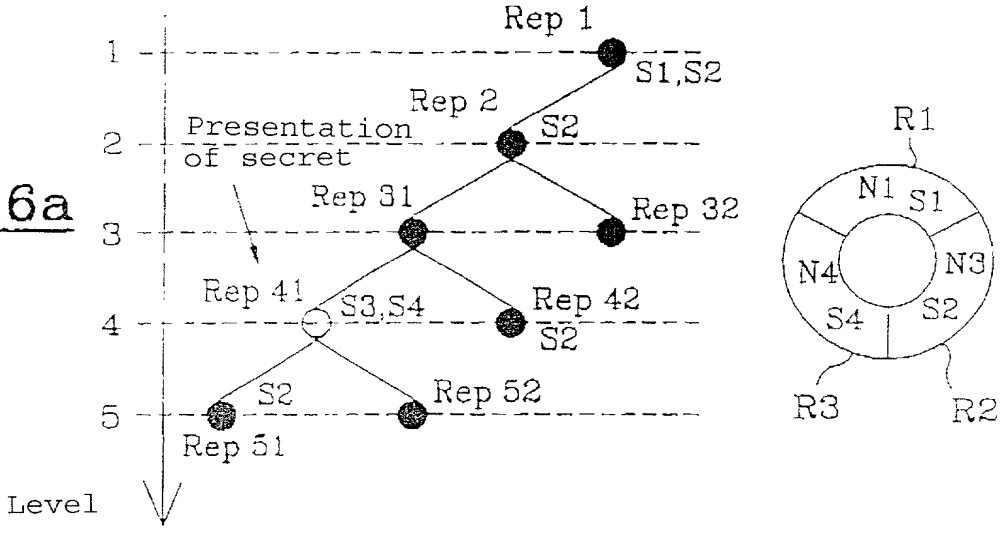


FIG.3.6b

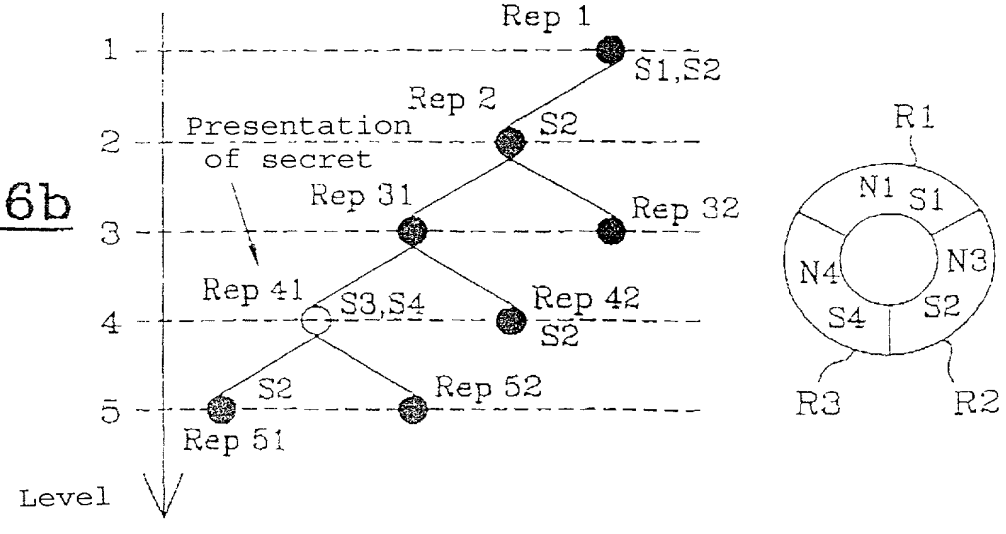


FIG.4.1

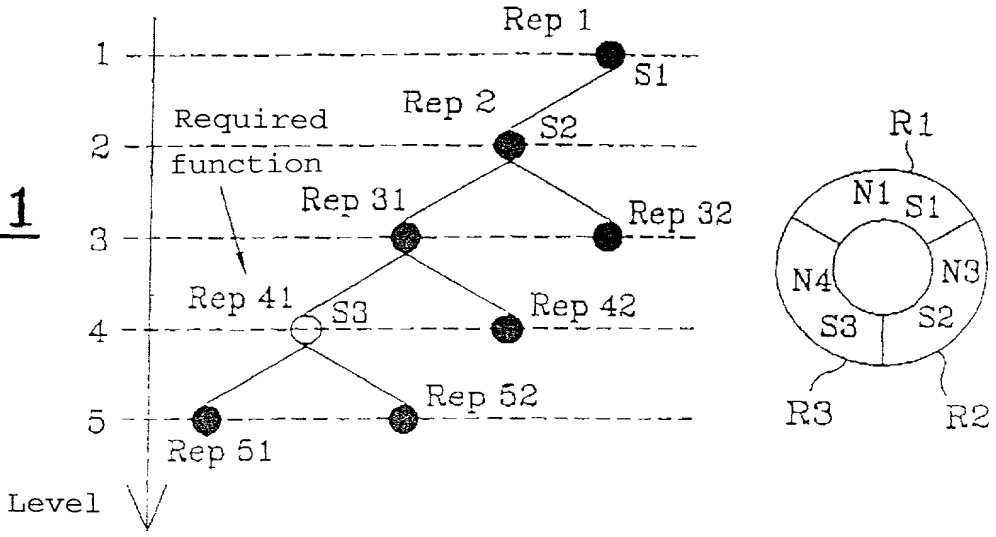


FIG.4.2

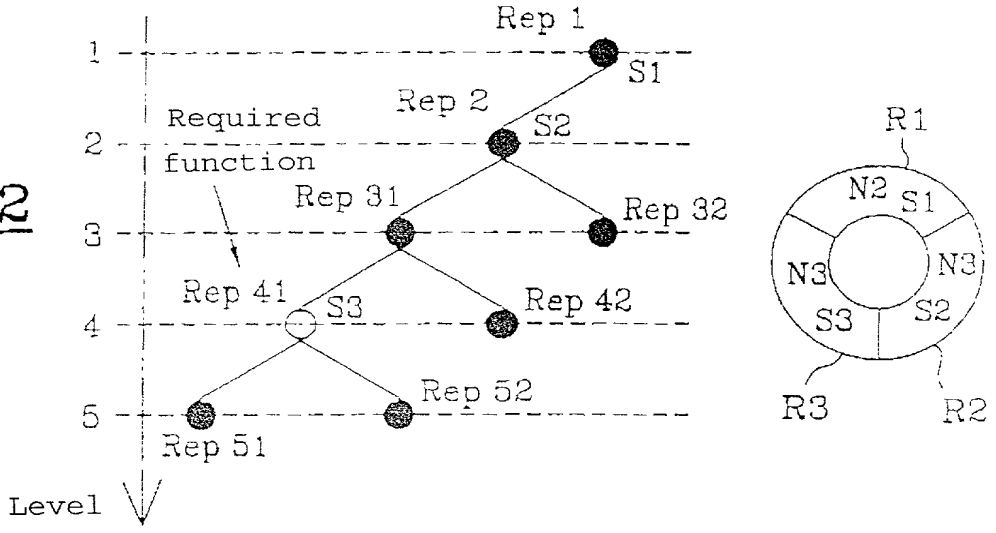


FIG.4.3

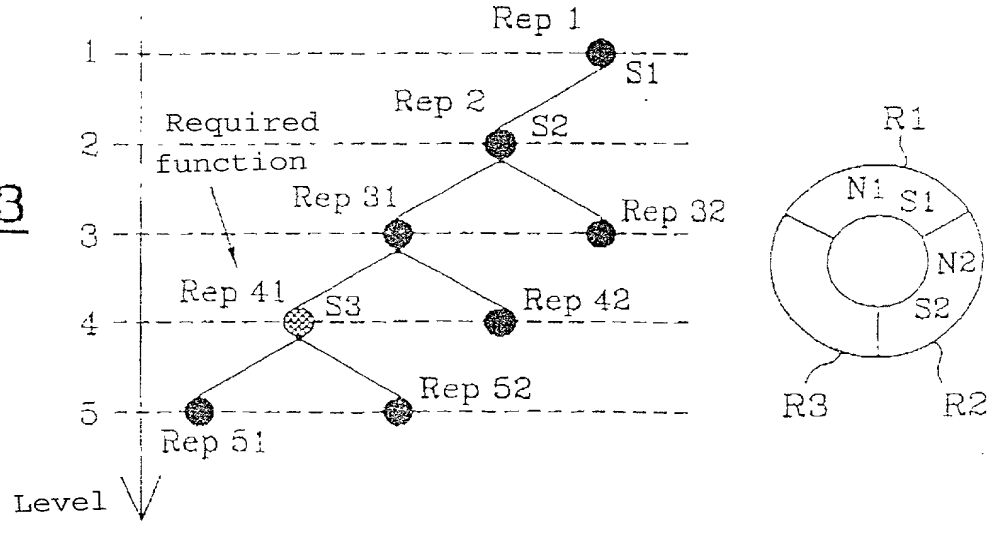


FIG.4.4

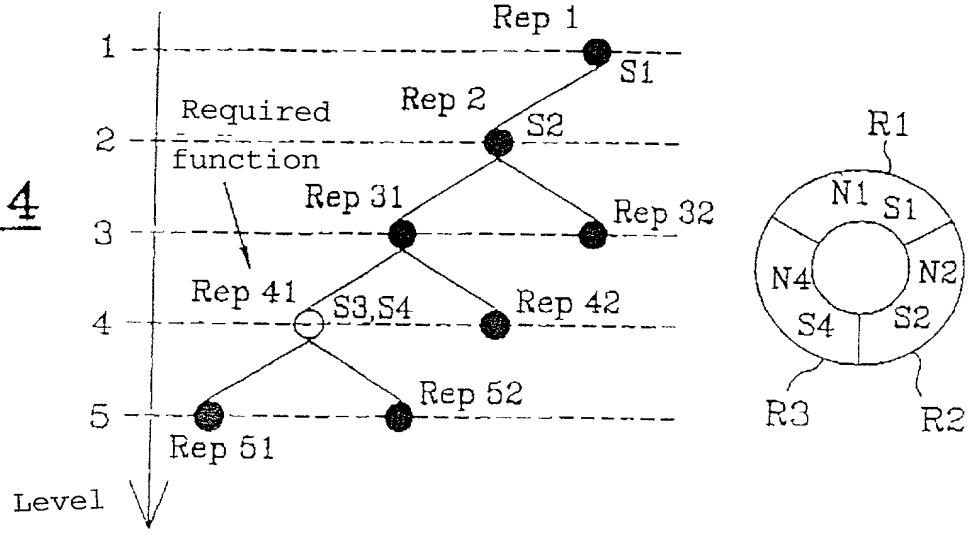


FIG.4.5

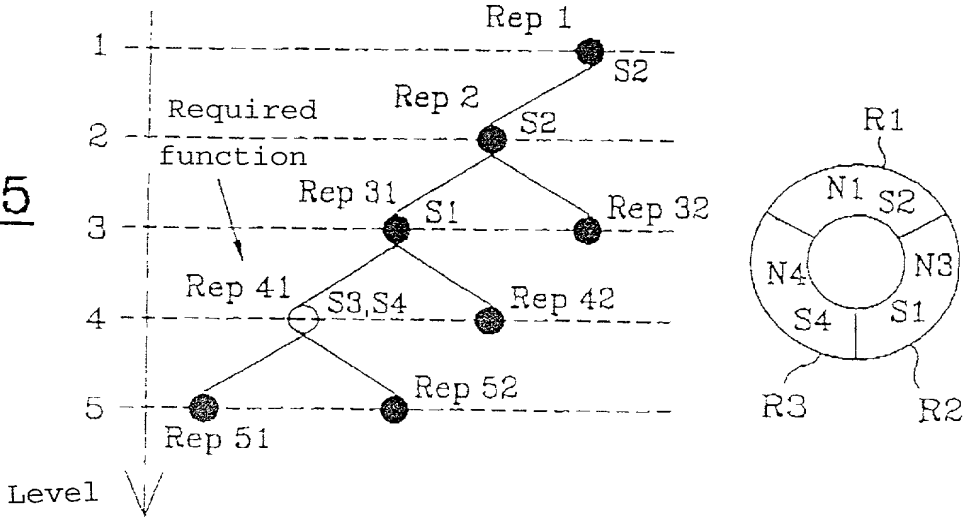
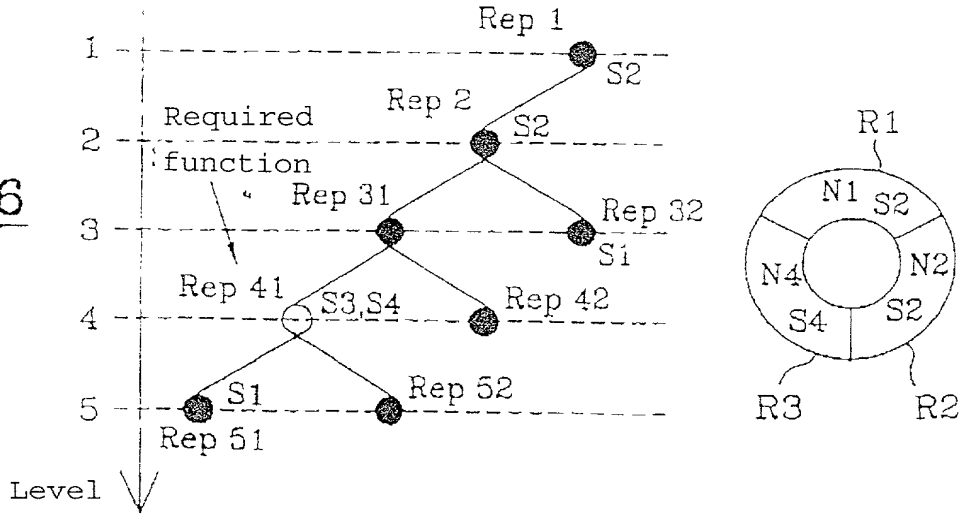


FIG.4.6



COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY **(Includes Reference to Provisional and PCT International Applications)**	Attorney's Docket No. 032326-080

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name;
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR MANAGING COMPUTER APPLICATIONS SECURITY

the specification of which (check only one item below):

☐ is attached hereto.

☐ was filed as United States application
Number _____
on _____
and was amended
on _____ (if applicable).

☒ was filed as PCT international application
Number PCT/FR99/00096
on 20 January 1999
and was amended
on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §119:

COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §119
France	98/01008	29 January 1998	X Yes _No
			_Yes _No
			_Yes _No
			_Yes _No
			_Yes _No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

_____ _____
(Application Number) (Filing Date)

_____ _____
(Application Number) (Filing Date)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) (Includes Reference to Provisional and PCT International Applications)	Attorney's Docket No. 032326-080

I hereby claim the benefit under Title 35, United States Code, §120 of any United States applications(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations §1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. §120:

U.S. APPLICATIONS		STATUS *(check one)*		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED

PCT APPLICATIONS DESIGNATING THE U.S.					
PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)			
PCT/FR99/00096	20 January 1999			X	

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	R. Danny Huntington	27,903	Gerald F. Swiss	30,113
Robert S. Swecker	19,885	Eric H. Weisblatt	30,505	Charles F. Wieland III	33,096
Platon N. Mandros	22,124	James W. Peterson	26,057	Bruce T. Wieder	33,815
Benton S. Duffett, Jr.	22,030	Teresa Stanek Rea	30,427	Todd R. Walters	34,040
Norman H. Stepno	22,716	Robert E. Krebs	25,885	Ronni S. Jillions	31,979
Ronald L. Grudziecki	24,970	William C. Rowland	30,888	Harold R. Brown III	36,341
Frederick G. Michaud, Jr.	26,003	T. Gene Dillahunty	25,423	Allen R. Baum	36,086
Alan E. Kopecki	25,813	Patrick C. Keane	32,858	Steven M. du Bois	35,023
Regis E. Slutter	26,999	Bruce J. Boggs, Jr.	32,344	Brian P. O'Shaughnessy	32,747
Samuel C. Miller, III	27,360	William H. Benz	25,952	Kenneth B. Leffler	36,075
Robert G. Mukai	28,531	Peter K. Skiff	31,917	Fred W. Hathaway	32,236
George A. Hovanec, Jr.	28,223	Richard J. McGrath	29,195		
James A. LaBarre	28,632	Matthew L. Schneider	32,814		
E. Joseph Gess	28,510	Michael G. Savage	32,596		

21839

and: _____

Address all correspondence to:

21839

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

Address all telephone calls to: James A. LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) (Includes Reference to Provisional and PCT International Applications)	Attorney's Docket No. 032326-080

FULL NAME OF SOLE OR FIRST INVENTOR Charles COULIER	SIGNATURE	DATE 22.08.2000
~~RESIDENCE~~ 19, avenue Frédéric Mistral, Le Cannet, F-13360 Roquevaire, FRANCE FRX	CITIZENSHIP French	
POST OFFICE ADDRESS 19, avenue Frédéric Mistral, Le Cannet, F-13360 Roquevaire, FRANCE		
FULL NAME OF SECOND JOINT INVENTOR, IF ANY Philippe BRUN	SIGNATURE	DATE 04.09.2000
RESIDENCE 14, allée du Ribas, Lotissement des Séveriers, F-13600 La Ciotat, FRANCE FRX	CITIZENSHIP French	
POST OFFICE ADDRESS 14, allée du Ribas, Lotissement des Séveriers, F-13600 La Ciotat, FRANCE		
FULL NAME OF THIRD JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		